# Navigacija kroz pejzaž internet prevara

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Andrijana Bosiljčić
mi231031@alas.matf.bg.ac.rs

Anđela Damnjanović
mi19059@alas.matf.bg.ac.rs

Igor Paunović
mi231040@alas.matf.bg.ac.rs

Luka Radanović
mi231010@alas.matf.bg.ac.rs

22. novembar 2023.

**Sažetak**

Pojava interneta omogućila je nikad lakše dolaženje do informacija i znanja, brže povezivanje ljudi koji dele slična interesovanja i još mnogo toga. Sa druge strane, ljudi su upravo u tim novim mogućnostima uvideli prostor za prevaru. Stoga su u ovom radu opisane najčešće vrste internet prevara, kao i načini na koje se one realizuju jer da bi se došlo do rešenja problema potrebno je dobro poznavati taj problem. Zatim je ukratko izloženo kako se zaštititi od prevara, kao i profili koji su podložniji da upadnu u zamku. Dodatno, navedeni su poznati primeri nekih internet prevara.

***Ključne reči*** — internet prevare, fišing, farming, krađa identiteta, lažno predstavljanje, romantične prevare, lažne internet prodavnice, nigerijska prevara, prevare starijih lica, prevare sa putovanjima, lutrijske prevare, prevare sa preplaćivanjem, prevare sa nasleđivanjem, prevare sa kriptovalutama, prevare sa kreditnim karticama, prevare pri konkurisanju za posao

## Sadržaj

# 1 Uvod

Pojava interneta donela je izuzetan napredak u komunikaciji, trgovini i razmeni informacija, ali i potencijalne opasnosti kao što su internet prevare koje predstavljaju rizik ne samo za pojedinca, već i za firme i društvo u celini. Uporedo sa razvojem tehnologije, sajber kriminalci upotrebljavaju sve sofisticiranije tehnike sa ciljem da ukradu nečiji identitet, lične podatke ili novac. Kako biste zaštitili sebe i svoje bližnje od internet prevara, u ovom radu ćemo prikazati koje sve vrste internet prevara postoje, kako se sprovode, kako se zaštiti od njih, kao i ko su najčešće žrtve.

# 2 Internet prevara - pojam i vrste

### 2.0.1 Internet prevara - pojam

Internet prevara predstavlja korišćenje internet usluga ili softvera sa internet pristupom s ciljem da se obmane pojedinac, organizacija ili firma radi finansijske dobiti ili nanošenja štete. Ovakve prevare predstavljaju najrasprostranjeniji oblik visokotehnološkog kriminala. U nastavku teksta biće navedene neke od najčešćih vrsta internet prevara [1].

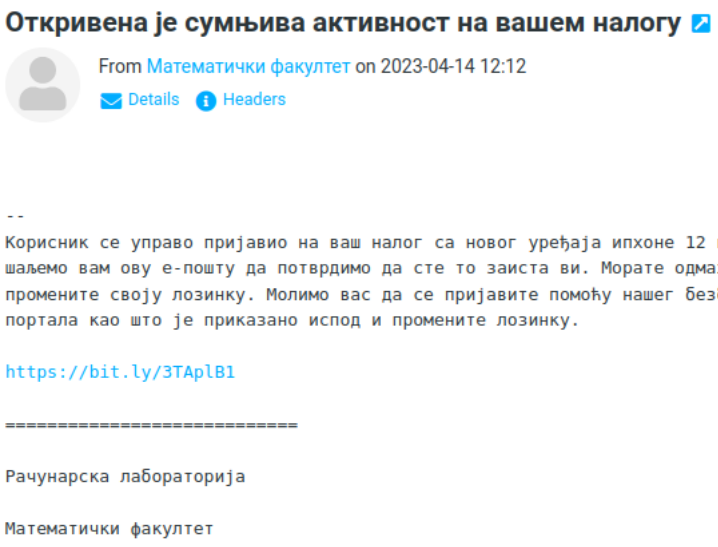
### 2.0.2 Internet prevare - vrste i način na koji se sprovode

**Fišing** (eng. *phishing*) je vrsta internet prevare u kojoj zlonamerni akteri pokušavaju da otkriju osetljive podatke pojedinca ili organizacije kao što su lični podaci, kredencijali za prijavljivanje na neki nalog, informacije o platnim karticama ili računu u banci [12, 28]. Prema podacima Federalnog istražnog biroa (eng. *Federal Bureau of Investigation*), 300.497 ljudi je postalo žrtva fišing prevara u 2022. godini. Zajedno su izgubili 52.1 milion dolara [16].

Fišing napadi se najčešće sprovode tako što sajber kriminalci kreiraju lažnu veb-stranicu, nakon čega pošalju žrtvama poruku elektronskom poštom sa adrese koja liči na legitimnu adresu kao što je adresa neke banke, društvene mreže ili internet prodavnice. U poruci se obično navodi da će žrtvi uskoro biti blokiran internet nalog ili platna kartica, pa čak i da će im sa računa biti skinuta određena suma novca, ali da je to moguće sprečiti klikom na link koji se nalazi u nastavku poruke. Upravo zbog načina na koji su ove poruke napisane žrtva često, ne želeći da joj se blokira nalog ili kartica, klikne na link koji je zatim vodi do pomenute lažne veb-stranice (koja veoma liči na stranicu banke ili internet prodavnice, ali se obično razlikuje u nekom karakteru), gde će biti zatraženo korisničko ime i lozinka. Kada dobiju tražene podatke, kriminalci mogu pristupiti nalozima svojih žrtava, ukrasti dodatne podatke ili čak pristupiti uređajima na koje su žrtve bile povezane, što im omogućava da izvrše prevare još većih razmera [16, 22, 23]. Na slici 1 može se videti pokušaj fišinga sproveden na Matematičkom fakultetu u Beogradu.

Takođe, postoje neetički ljudi koji koriste prilike i sprovode prevare u slučajevima kada se desi neka prirodna katastrofa. Oni šalju mejl poruke predstavljajući se kao legitimne dobrotvorne ili vladine organizacije i pokušavaju da ubede žrtvu da donira novac. Oni mogu da koriste kreditnu karticu i lične podatke žrtve u razne svrhe [10, 22].

**Farming** (eng. *pharming*) je vrsta internet prevare koja podseća na fišing, ali ih ne treba mešati. U nastavku su date dve vrste farming napada




Slika 1: Primer pokušaja fišinga na Matematičkom fakultetu

[2, 18].

- **Farming zasnovan na zlonamernom softveru** javlja se jer korisnici interneta često nesvesno preuzimaju zlonamerni softver (eng. *malware software*) putem poruke elektronske pošte poslate sa lažne adrese ili preuzimanja nekog softvera. Nakon preuzimanja zlonamernog softvera, korisnik biva trajno preusmeren na lažnu veb-adresu koju je napadač prethodno kreirao. Svaki put kada neko od korisnika pristupi toj adresi, napadači vide sve podatke koje korisnik unosi. Ovde se mogu ubrajati i prevare tehničke prirode gde žrtva dobija iskačuće upozorenje na veb stranici koja je u vlasništvu prevaranata i koji ukazuju na to da im je računar zaražen. Sprovodi se tako što prevaranti traže od žrtve da preuzme aplikaciju koja im omogućava da daljinski kontrolišu računar žrtve kako bi rešili problem. Oni zatim preuzimaju stvarni virus ili žrtvu na neki drugi način navode da veruje da još nešto nije u redu i kažu da mogu da reše problem uz novčanu nadoknadu [16, 2].
- **Trovanje DNS servera** uključuje manipulacije DNS-om (eng. *Domain name system*, sistemom imena domena) kako bi se posetioci veb-adrese preusmerili na lažne veb-lokacije. Za razliku od napada zasnovanim na zlonamernom softveru, ovi napadi utiču na širu publiku manipulisanjem infrastrukture interneta (napadači manipulišu DNS tabelama koje žrtve zatim preusmeravaju na lažne adrese), što znači da i korisnici koji unesu tačnu adresu veb-lokacije u svojim pretraživačima mogu biti preusmereni na lažnu veb-adresu bez njihovog znanja [2].

**Lažne internet prodavnice** — Onlajn kupovina donela je razne pogodnosti kao što je kupovina u bilo koje doba dana, lako upoređivanje cena [25], ali je sa sobom donela i rizik od prevara. Napadači koji se odluče da izvrše ovakve prevare kreiraju lažne veb-sajtove za kupovinu

koji ili izgledaju originalno ili repliciraju postojeće veb-sajtove prodavaca. Imaju URL adrese slične brendovima koje pokušavaju da oponašaju (npr. Amaz0n.net). Obično sadrže ponude koje su previše dobre da bi bile istinite, npr. ponude popularnih brendova po veoma niskim cenama. Napadači to koriste da prevare žrtve i zabeleže podatke o bankovnom računu u trenutku kupovine [16].

**Romantične prevare** — internet prevara koja podrazumeva da prevaranti kreiraju lažne naloge na sajtovima za upoznavanje preko kojih u relativno kratkom vremenskom periodu izražavaju snažne emocije prema žrtvi, uz predlog da komunikaciju nastave preko mejla, SMS poruka ili slično. Prevarant nakon određenog vremena traži novac, poklone, čak i lične informacije od žrtve [7, 9, 23].

**Lažno predstavljanje** (eng. *catfishing*) je vrsta internet prevare gde osoba stvara lažni identitet na nekoj od društvenih mreža, obično ciljajući određenu žrtvu, sa željom da od nje iznudi novac [24].

Primer je romantična prevara 2.0.2 . Kada napadači steknu poverenje žrtve, od nje traže poklone, novac, podatke o bankovnom računu, često izmišljajući razloge za to (npr. trenutno su u lošoj finansijskoj situaciji, imaju porodičnih problema, treba im pozajmica, žele da prenesu novac van zemlje, ali im je za to potreban novac za plaćanje poreza ili taksi)[24].

Takođe, često se dešava da žrtva želi da kupi neki artikal, npr. automobil i u tom cilju kontaktira osobu koja je postavila oglas. Ako je ta osoba prevarant, onda šalje žrtvi lažne lične podatke i lažni dokaz o vlasništvu automobila. Pod izgovorom da živi u inostranstvu govori da mu je lakše da komunikacija bude preko elektronske pošte ističući popularnost oglasa i da ako žrtva odmah uplati novac dobija popust, a sve sa ciljem da se žrtva brzo odluči za kupovinu [6].

Poznat primer lažnog predstavljanja : Mantaj Teo, istaknuti univerzitetski igrač američkog fudbala, dospeo je 2012. godine na naslovne strane kada je otkriveno da je naseo na prevaru od strane Lenej Kekue, ličnosti koju je izmislio Ronaja Tuisusopo, koji je koristio lažni profil na društvenim mrežama kako bi uspostavio vezu sa Teom. Čak je izmislio i njenu smrt kako bi stekao njegove simpatije. Po ovom događaju je snimljen film "Devojka koja nije postojala" [24].

**Prevare starijih lica** — internet prevaranti znaju da su starije osobe ranjivije kada je u pitanju internet i to koriste kako bi ih prevarili [7].

Postoje razni načini na koje se stariji mogu obmanuti. Jedan od njih su romantične prevare 2.0.2 koje podrazumevaju da se napadači predstavljaju kao potencijalni partneri starijim ljudima koji su u potrazi za životnim saputnikom da bi im na kraju tražili novac za različite svrhe.

Zatim, postoje i napadači koji se predstavljaju kao tehnička podrška i nude svoje usluge kako bi popravili nepostojeće kvarove na računaru [11]. Na ovaj način napadači dobijaju pristup ličnim podacima žrtava.

Ne treba izostaviti ni prevare u kojima napadači stupaju u kontakt sa starijima predstavljajući se kao član porodice da bi tražili da im se na račun uplati novac [7, 11, 16].

**Nigerijska prevara** — Ova prevara poznata je i pod nazivom "Prevara 419". „Nigerijska prevara" najšešće počinje tako što žrtva dobija poruku elektronskom poštom, koja obično sadrži lažne informacije o dobicima u igrama na sreću, prikupljanju sredstva u dobrotvorne svrhe ili nasleđu imovine preminulih osoba, najčešće daljih rođaka. Zatim napadači ubeđuju žrtve da učestvuju u podeli novca, pri čemu žrtve moraju unapred da uplate određeni novčani iznos. Pošto je iznos koji treba uplatiti znatno manji od potencijalnog dobitka, žrtve se opredeljuju za ovaj korak. Na-

kon toga, elektronskom porukom (najčešće „spam“ (eng. *spam*) porukom (još jedna vrsta internet prevare) poslatom iz internet kafea) od primaoca poruke se traži pomoć pri transferu novčanih iznosa koji se kreću od par stotina hiljada do par desetina miliona dolara za koji će, nakon obavljenog transfera, žrtva dobiti određeni procenat kao nadoknadu (procenat zarade koji se obećava kreće se i do 40% od sume novca koja je predmet posla). Ukoliko žrtva odgovori na prvu poruku, napadači pokušavaju da je izmanipulišu da otkrije poverljive informacije o sebi tako što ubeđuju žrtvu da je baš njena pomoć neophodna da bi se posao završio. Kada žrtva uplati traženi iznos, napadači pod raznim izgovorima odlažu isplatu koju su obećali u zamenu za pomoć. Sa druge strane, oni nastavljaju da od žrtve traže novac pod izgovorom da i dalje postoje takse koje treba platiti da bi se pokrili dodatni administrativni troškovi, obećavajući opet da će žrtva dobiti svoj deo u najkraćem roku. Naravno, kada žrtva uplati i novi iznos, opet ulaze u isti začarani krug odlaganja isplate i traženja novca od žrtve [17].

**Putovanja** — ova vrsta prevare se uglavnom dešava na društvenim mrežama. Prevaranti kače primamljive slike predela na društvene mreže i navodno nude besplatne karte ili putovanja na te destinacije. Od korisnika se samo traži da popuni anketu. Međutim, te ankete traže od korisnika dosta ličnih podataka. Neki prevaranti čak i kreiraju lažne veb-sajtove (koji dosta podsećaju na prave, legitimne sajtove) na kojima je moguće izvršiti rezervacije. Takođe, moguće je i prodavanje lažnih polisa osiguranja [6].

**Lutrijske prevare** podrazumevaju da prevaranti šalju lažne elektronske ili tekstualne poruke kojima obaveštavaju žrtve da su osvojili nagradu na lutriji. Da bi dobili svoju nagradu, žrtvama se traži da uplate razne troškove ili da pošalju informacije o bankovnom računu. Ovo može biti vrsta fišing napada 2.0.2, jer se može desiti da žrtve budu upućene na lažne veb lokacije ili da dostave lične i finansijske podatke [7, 21].

**Prevare sa preplaćivanjem** — u svom najosnovnijem obliku, kada praktikuju ovu vrstu prevare napadači lažno tvrde da je žrtvi uplaćeno više novca nego što je trebalo, te se od žrtve zahteva da vrati razliku između uplaćenog novca i dogovrenog iznosa. Ova prevara može imati više oblika [7].

- **Prevara sa lažnim čekovima** je jedna vrsta prevare sa preplaćivanjem. Žrtve ove prevare mogu biti osobe koje prodaju artikle preko interneta ili nekog oglasa. Analogno osnovnom obliku prevare sa preplaćivanjem, prevarant želi da kupi određeni proizvod dajući lažni ček na kome je napisan iznos veći od dogovorenog, nakon čega traži od žrtve da mu vrati preostali novac. Ubrzo nakon slanja novca, žrtva saznaje da je prevarena [7, 20].
- **Prevara sa povraćajem novca** je vrsta internet prevare u kojoj prevaranti zovu ljude nasumično dok ne nađu žrtvu koja će im poverovati. Prevarant se predstavlja kao osoba iz firme koja žrtvi treba da vrati novac jer žrtva nije dobila određeni proizvod. Zatim od žrtve traži da mu omogući pristup računaru preko softvera i da se prijavi na veb-stranicu za online bankarstvo. Prevarant isprazni ekran pomoću softvera za udaljen pristup i pomoću alata za razvoj veba u pretraživaču žrtve da privremeno uredi veb-stranicu za internet bankarstvo kako bi prikazao da je novac koji je uplaćen na nalog žrtve veći od očekivanog. Prevarant ubeđuje žrtvu kako će posao firme biti ugrožen ukoliko ne uplati višak novca. Povraćaj novca se vrši bankovnim transferom, novčanom uplatnicom ili poklon karticom. Tek

nakon određenog vremenskog perioda žrtva saznaje da je prevarena (obično nakon sto uđe ponovo na veb-stranicu internet bankarstva). Ovo je takođe i vrsta tehničke prevare jer prevarant obično prati isti format povezivanja sa računarom žrtve (preko softvera za udaljeni pristup). Dešava se i da žrtva dobije poruku elektronskom poštom u kojoj prevarant moli za pomoć prenosa ogromne količine novca u inostranstvo ili traži podatke o bankovnom računu žrtve kako bi obavio transakciju obećavajući im novac zauzvrat [7].

**Prevare sa nasleđivanjem** — prevaranti koji se odluče za ovu vrstu prevare kontaktiraju žrtvu predstavljajući se kao advokati i obaveštavaju žrtvu da joj je ostavljeno veliko nasledstvo od rođaka ili nekog bogatog dobrotvora koji je preminuo u inostranstvu. Da bi prevara bila verodostojnija, prevaranti mogu da pristupe javnim podacima o žrtvi i da nađu informacije o preminulima u njenoj okolini, ali se dešava i da samo izmisle ime preminulog. Oni zatim ubeđuju žrtvu da je potrebno da plati razne vrste troškova i da popuni formular dajući lične podatke kako bi dobila nasledstvo [7].

**Konkurisanje za posao** — poslednjih nekoliko godina došlo je do povećanja broja kandidata koji traže radna mesta koja nude rad od kuće. Prevaranti su toga svesni i ciljne grupe su im upravo ti ljudi.Prevara obično uključuje ubeđivanje žrtve da kupi neke stvari ili uplati naknadu (npr. ukoliko pozicija zahteva podnošenje početne takse za registraciju) uz obećanje provizija ukoliko namame i druge osobe da se prijave. Prevaranti nude žrtvama "informativni materijal" koji će im omogućiti da se pripreme i lako dobiju posao u određenoj kompaniji, a zauzvrat traže novac. Zatim se žrtva obaveštava da je izabrana kao jedan od finalista za određenu poziciju (obično žrtva nije ni konkurisala za posao). Kada dođe vreme za intervju, prevarant otkriva da je to online intervju putem određene usluge za razmenu poruka, koja od žrtve traži da unese lične podatke kojima prevarant tada može da pristupi [15].

**Prevare sa kriptovalutama** — da bi vršili prevare sa kriptovalutama [29], napadači kreiraju lažne platforme za trgovanje kriptvalutama ili lažne verzije zvaničnih kripto novčanika (koje izgledaju slično legitimnim sajtovima). Lažni kritpo-sajtovi uglavnom rade na dva načina, kao fišing stranice i kao jednostavna prevara [16].

- **Fišing stranice** — upotrebom fišing stranica, prevaranti imaju mogućnost da vide sve podatke (lozinka kripto-novčanika, lični i finansijski podaci) koje žrtva unese [16].
- **Jednostavna prevara** sa druge strane, u početku omogućava žrtvi da podigne malu količinu novca. Ako žrtva vidi da investicije imaju dobre rezultate ona ulaže dodatni novac, međutim kada posle određenog vremena pokuša da podigne novac sajt se ili gasi ili odbija zahtev [16].

**Krađa identiteta** podrazumeva nezakonito pribavljanje i korišćenje tuđih ličnih podataka u razne svrhe (za dobijanje kredita ili novca, kupovinu proizvoda, sumnjive transakcije sa računa). Ova vrsta prevare dešava se uglavnom na društvenim mrežama, gde prevarant kopira sliku profila i lične podatke žrtve koje su javno dostupne i pravi lažni nalog koji koristi u različite svrhe. Zatim, u cilju dolaženja do dodatnih informacija, šalje zahteve profilima koje žrtvin originalni profil prati [27]. Takođe se dešava da prevaranti pogode lozinku žrtve pomoću algoritama koji mogu da pogode milijarde lozinki u sekundi, čime dolaze do ličnih podataka žrtve. Nakon dobijanja podataka o identitetu, napadači mogu da koriste žrtvin

račun u banci, prave nove račune na lažno ime, vrše transakcije na svoje račune i kupuju proizvode novcem žrtve. Ovo predstavlja i vrstu krađe identiteta. Ovde takođe treba navesti i prevaru internet bankarstva koja je česta pojava. Prevaranti korišćenjem onlajn tehnologije nezakonito izvlače novac sa bankovnog računa žrtve i vrše transfer novca na svoj račun [16, 22].

**Prevara sa kreditnim karticama** odnosi se na bilo kakvu neovlašćenu upotrebu kreditne, debitne kartice ili sličnog načina plaćanja za kupovinu proizvoda ili usluga bez ovlašćenja vlasnika kartice. Ovo ne zahteva fizičko posedovanje kartice žrtve i može se uraditi pristupom broju kreditne kartice, datumu isteka i CCV broju. Prevara sa kreditnim karticama se često dešava nakon uspešnog okončanja druge vrste internet prevare gde se dobijaju podaci o kartici [7].

# 3 Žrtve internet prevara

Možda iznenađujuće, podaci Savezne trgovinske komisije (FTC) iz 2021. [5, 8] pokazuju da su u SAD osobe od 18 do 59 godina generalno češće prijavljene kao žrtve prevara nego one od 60 i više. Ipak, postoje velike razlike u žrtvama u zavisnosti od vrste prevare. Na primer, mlađe osobe su bile znatno podložnije prevarama vezanim za onlajn kupovinu, zapošljavanje i investiranje (naročito u kriptovalute). Sa druge strane, starije osobe su češće bile žrtve nagradnih igara, lutrija, i prevara tehničke podrške. Poslednja stavka se može dovesti u vezu sa njihovim obično znatno slabijim tehničkim znanjem. Iako su se ređe javljali kao žrtve prevara, starije osobe su imale drastično veće središnje vrednosti gubitka, oko 800 dolara za one od 70 do 79 godina, a za one preko 80 godina čak i 1500 dolara, dok je za mlađe osobe središnja vrednost gubitka bila 500 dolara. Još jedna velika razlika je u mestu na kom su osobe prevarene. Prevaranti su češće stizali elektronskom poštom do starijih nego do mlađih, dok su društvene mreže češće bile mesto prevara za mlađe osobe nego za starije.

S obzirom na to da veliki broj ljudi provodi dosta vremena na društvenim mrežama, koje se često javljaju kao mesto prevara, može se postaviti pitanje koji faktori utiču na podložnost osoba na ove prevare [30].

Jedno istraživanje iz 2015. godine [30] se upravo bavilo uticajem navika i ponašanja studenata na Fejsbuku na rizik da budu prevareni fišing napadom. Za osobe koje su mnogo vremena provodile na Fejsbuku i nisu mogle da iskontrolišu dužinu provedenog vremena, postojala je dosta veća verovatnoća da prihvataju zahteve za prijateljstvo od nepoznatih ljudi. Takođe, osobe koje su se osećale pod društvenim pritiskom da uzvrate zahtev za prijateljstvo su ga mnogo češće prihvatale, dok su osobe koje se više brinu za svoju privatnost bile pod manjim rizikom prihvatanja.

Ono što je istraživanje takođe pokazalo jeste da je za osobe sa uobičajenom navikom da provode puno vremena na Fejsbuku postojala veća verovatnoća da odgovaraju na poruke od nepoznatih ljudi na Fejsbuku (u istraživanju su studenti dobijali poruku od osobe koja se predstavljala kao poznanik nekog kome trebaju studenti za praksu, i tražila pojedine lične informacije). Postoji mogućnost da je veliki broj prijatelja na Fejsbuku koji su ove osobe imale, kao i navika na često korišćenje doprinele da previde neke detalje poruke ili pomisle da je od prijatelja bez da razmišljaju odakle ga poznaju i kako su došli do toga da budu povezani na Fejsbuku, zbog čega završe kao žrtva fišinga.

U prethodnom primeru, kao i često u drugim fišing prevarama, dolazi

do tzv. perifernog procesiranja informacija [30, 13], gde osoba iz dobijene poruke ne zaključuje o njoj prvenstveno na osnovu njenog sadržaja i činjenica, već na osnovu načina na koji je prezentovana.

Vršena su istraživanja u cilju pokazivanja koje osobine ličnosti utiču na to da će verovatnije procesirati informacije iz fišing poruka na ovaj način i samim tim imati veći rizik da budu njegove žrtve [13]. Pokazalo se da osobine koje su otvorenost, saradljost ili neuroticizam imaju pozitivan uticaj i na periferno i na centralno procesiranje. Pokazalo se da savesnost ima negativan uticaj na periferno procesiranje, pa se smatra da će savesne osobe lakše prepoznati fišing prevaru. Ekstraverzija nije imala statistički značajan uticaj ni na periferno ni na centralno procesiranje.

Jedno anketiranje koje se bavilo utvrđivanjem uticaja karakteristika osoba na njihovu podložnost internet prevarama je rađeno 2020. i obuhvatalo je preko 10.000 osoba sa područja Ujedinjenog Kraljevstva [31]. Lokus kontrole se pokazao kao uticajan na podložnost prevarama. Naime, osobe koje veruju da imaju kontrolu nad tokom svog života su češće bile prevarene. To se može objasniti time što zbog sigurnosti u sebe zanemaruju uticaj koji prevaranti mogu imati na njihove odluke. Suprotno od očekivanog, pokazalo se da su muškarci i edukovane osobe češće bili žrtve. Takođe, žrtve prevara sa ulaganjem su češće bili stariji i muškarci. Sa druge strane, žrtve prevare potrošača su uglavnom bile žene i manje edukovane.

Sva ova istraživanja o žrtvama su veoma značajna, jer nam mogu dati značajne informacije koje se kasnije mogu koristiti za razumevanje mehanizama prevara u cilju borbe protiv njih, kao i u osmišljavanju programa obuke i edukacije osoba na temu internet bezbednosti [32, 8]. Zbog toga je važno da internet prevare budu prijavljene, tako da bi mogla da se stekne što realnija slika o ovom problemu. Prema podacima iz različitih godina (2005, 2011, 2017) [4] oko 45% žrtava se žalilo nekome osim svoje porodice i prijatelja. Razlike postoje u procentima vezanim za konkretne prevare: osobe kojima je naplaćen proizvod koji nisu pristali da kupe su se znatno češće žalile (60%) nego, na primer, osobe koje su platile lažnu popravku računara (20%). Žrtve su se najviše žalile prodavcu ili proizvođaču proizvoda (30%), manje njih banci ili pružaocu platnih usluga (12%), a državnim institucijama samo oko 3%.

# 4 Kako se ljudi mogu zaštiti od internet prevara?

Postoje različiti, tehnički ili netehnički, načini da se spreče internet prevare.

U netehničke načine spada edukacija, razumevanje kako odredeni napadi funkcionišu, kao i uvid u raznovrsnost internet prevara. Iako se ovo često uzima zdravo za gotovo, važno je shvatiti da su upravo sami korisnici prva linija odbrane od internet prevara. U tabeli 1 dat je pregled najopštijih tehnika zaštite od prevara.

Pored nabrojanih netehničkih metoda, postoje i razni tehnički načini zaštite od posebnih vrsta prevara. Tako se u tabeli 2 mogu naći informacije kako se zaštititi od fišing napada, u tabeli 3 su navedene smernice za zaštitu od farminga, a u tabeli 4 od lažnog predstavljanja.

Detektovani fišing sajtovi se mogu blokirati i na taj način se ne mogu koristiti za prevaru. Iako je relativno lako manuelno proveriti da li je veb-sajt fišing ili ne, automatsko lociranje ovih veb-sajtova predstavlja znatno

Tabela 1: Pregled opštih metoda zaštite od internet prevara

| Tehnika | Opis tehnike |
|---|---|
| Promena lozinke | Redovno menjati lozinke |
| Jedinstvenost lozinke | Posebna lozinka za svaki nalog |
| Dvofaktorska autentikacija | Korišćenje dvofaktorske autentikacije |
| Kritičko razmišljanje | Doza nepoverenja za ponude koje zvuče previše dobro da bi bile istinite |

Tabela 2: Tehničke metode zaštite od fišing napada

| Tehnika | Opis tehnike |
|---|---|
| Detekcija fišing sajta | Ručna provera verodostojnosti veb-sajta |
| Poboljšanje sigurnosti | Korišćenje biometrike ili dodatnih hardverskih uređaja |
| Korišćenje spam filtera | Provera da li je server sa koga je poruka poslata autorizovan |
| Anti fišing softver | Provera da li je veb-sajt u bazi fišing veb-sajtova |

teži posao.
Zato ljudi koji ordžavaju originalni veb-sajt često sprovode aktivnosti praćenja kako bi identifikovali potencijalne pretnje, poput neovlašćenih domena koji su slični njihovom, putem provere baza registracije domena, izvršavanja DNS upita i korišćenja specijalizovanih alata. Na primer, *www.1cbc.com.cn* može biti domen lažnog sajta, dok je domen originalnog veb-sajta *www.icbc.com.cn*.
Pošto napadač često želi da duplira sadržaj čitavog veb-sajta, može koristiti i različite alate da automatski preuzme veb stranice sa određenog sajta. Ovakva preuzimanja moguće je detektovati i pratiti, pa na taj napadač može biti identifikovan. Oba pristupa imaju svoje nedostatke [19].

Biznis veb-sajtovi, poput veb-sajtova banaka, mogu pribeći nekoj od novih metoda za garanciju bezbednosti korisničkih informacija. Tako Barkli banka daje čitač kartica svojim korisnicima. Pre kupovine, korisnici moraju da ubace karticu u čitač i ukucaju svoj lični pin kod, nakon čega se generiše jednokratna šifra. Korisnik može obaviti transakciju jedino ako ukucava tačnu šifru. Kompanija Paypal pokušala je da uz uobičajeno unošenje šifre dodatno uključi i prepoznavanje glasa, i tako dodatno unapredi bezbednost korisnika. Sa ovim metodama, koje su primeri dvofaktorske autentikacije, napadač ne može naneti štetu čak iako je došao do osetljive podatke. Mana ovih pristupa je povećavanje troškova i usložnjavanje cele infrastrukture, te je potrebno još vremena da se ove tehnike šire prihvate [19].

Napadači često koriste slabost SMTP (eng. *Simple Mail Transfer Protocol*) protokola za slanje elektronske pošte. Kako njemu fale mehanizmi autorizacije, informacije pošiljaoca, kao i rute preko kojih je poruka isporučena mogu biti lažirane u ovom protokolu. Zato napadači mogu poslati velike količine fišing mejlova sa lažne imejl adrese. Ako bi anti-spam sistem mogao da utvrdi da li je imejl zaista poslat sa naznačene adrese, učestalost

fišing napada bi drastično opala. Tehnike koje sprečavaju pošiljaoca da falsifikuju mejl se sastoje iz proveravanja da li je mejl poslat sa servera koji je autorizovan da šalje mejlove sa tog domena, i ako nije, mejl se označava kao spam. Iz ove perspektive, fišing mejlovi su tip spam mejlova [19].

Tabela 3: Tehničke metode zaštite od lažiranja DNS-a

| Tehnika | Opis tehnike |
|---|---|
| Provera sigurnosti konekcije | Proveriti da li je protokol https i ima li katanca ispred URL-a |
| Korišćenje VPN-a | Konektovati se na privatni DNS server |
| Biti obazriv | Ne kliktati na sumnjive linkove |
| Autentifikacija DNS ulaza | Podesiti DNSSEC |
| Kritičko razmišljanje | Doza nepoverenja za ponude koje zvuče previše dobro |
| Koristiti antivirus i antimalver | Instalitrati i koristiti programe koji služe za zaštitu računara |

Sigurnost konekcije može se lako proveriti. Na primer, na Google Chrome pretraživaču vidimo sivi katanac ispred URL-a koji označava sigurnu konekciju. Često nas veb pretraživač obavesti da konekcija nije sigurna, ovo obaveštenje ne treba ignorisati. Ipak, ovo nije dovoljan dokaz da je veb-sajt pravi, jer ovi veb-sajtovi mogu imati SSL/TLS sertifikate i koristiti https protokol [26].

Još jedna mera zaštite jeste povezivanje na privatni DNS server koji koristi enkripciju sa kraja na kraj i otporniji je na trovanje DNS-a. Takođe, može se podesiti i DNSSEC, koji radi tako što dodeljuje digitalne potpise DNS podacima i analizira sertifikate korenog domena da bi se uverio da su svi odgovori autentični. Ovo osigurava da svaki DNS odgovor dolazi sa originalne veb stranice. Nažalost DNSSEC nije u široj upotrebi, pa DNS podaci često ostaju neenkriptovani [26].

Tabela 4: Tehničke metode zaštite od lažnog predstavljanja

| Tehnika | Opis tehnike |
|---|---|
| Provera ispravnosti podataka | Korišćenje servisa koji mogu pomoći pri otkrivanju profila |
| Ne deliti lične informacije | Ne deliti lične informacije sa nepoznatim ljudima |
| Proveriti profilnu sliku | Koristiti alate koji vrše obrnutu pretragu slike |
| Zatražiti video poziv | Ako se sumnja u identitet osobe, zatražiti video poziv |

Postoje servisi kao što su Information.com i Instant Checkmate, koji mogu pomoći pri otkrivanju profila na društvenim mrežama, vesti i artikala gde su pominjani, njihovo radno mesto, odakle dolaze, ili bilo kog drugog sadržaja koji sadrži njihovo ime [3].

Čak i ako se ne upotrebi ova vrsta provere, treba znati da nikako ne treba deliti lične podatke sa nepoznatim osobama [14]. Zato, ako osoba počne da se raspituje o našim ličnim podacima, poput adrese, detalja našeg naloga ili o našem životu, moguće da je u pitanju prevara. Ako traže šifru zbog dodatne sigurnosti, uzbune ili nekakve potvrde, skoro uvek je prevara u pitanju. U redu je interagovati sa novim ljudima i stvarati nove prijatelje, ali uvek treba biti na oprezu i obratiti pažnju na znake prevare [3].

Takođe, ako je osoba sa kojom se dopisujemo sumnjiva, dobra ideja je da pretražimo slike koje osoba koristi jer ih je relativno lako identifikovati. Alati koji omogućavaju ovakve pretrage omogućavaju da potvrdu autentičnosti slike, kao i nalaženje originalne verzije. Primer takvog alata je TinEye[3].

Na kraju, jedan od najbržih načina za detekciju lažnog jeste zahtevaje video poziv. Izgovori poput onog da nemaju kameru podižu sumnje [3].

# 5 Zaključak

Kao što je u radu i izloženo, postoji mnogo vrsta internet prevara, a još više načina na koje korisnici mogu biti obmanuti. Poražavajuća statistika pokazala je da nijedan korisnik interneta nije imun na prevare, tj. za svakoga, nezavisno od pola, godina i zrelosti postoji prevara na koju bi mogao da nasedne. Stoga se treba neprestano edukovati, biti veoma oprezan pri komunikaciji sa nepoznatim ljudima, menjati šifre redovno, te ne deliti lične podatke ni sa kim. Međutim, kako je tehnologija u stalnom razvoju, izvesno je da će prevaranti pronalaziti sve inovativnije načine da dođu do zarade. Upravo zbog toga, odbrana od internet prevara će biti izazov dok god se tehnologije i ljudski um razvijaju.

# Literatura


[1] Sajber kriminal. on-line at: https://vokabezbedno.weebly.com/sajber-kriminal/internet-prevare.

[2] Abnormal. What Is Pharming? How DNS Spoofing and Malware Sends Users To Fake Websites? on-line at: https://abnormalsecurity.com/glossary/pharming.

[3] Cyber Management Alliance. 6 Ways to Protect Yourself From Online Catfishing. on-line at: https://www.cm-alliance.com/cybersecurity-blog/6-ways-to-protect-yourself-from-online-catfishing.

[4] Keith B Anderson. To whom do victims of mass-market consumer fraud complain? *Available at SSRN 3852323*, 2021.

[5] Federal Trade Commission. Who experiences scams? A story for all ages - Federal Trade Commission, 2022. on-line at: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages.

[6] European consumer centre France. Online fraud. on-line at: https://www.europe-consommateurs.eu/en/shopping-internet/internet-fraud-and-scams.html.

[7] Anti cybercrime group. COMMON TYPES OF INTERNET FRAUD SCAMS. on-line at: https://acg.pnp.gov.ph/main/cyber-security-bulletin/2-uncategorised/172-common-types-of-internet-fraud-scams.html.

[8] Marguerite DeLiema and Paul Witt. Profiling consumers who reported mass marketing scams: demographic characteristics and emotional sentiments associated with victimization. *Security Journal*, pages 1–44, 2023.

[9] FBI. Romance Scams, 2022. on-line at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/romance-scams.

[10] FBI. Charity and Disaster Fraud, 2023. on-line at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/charity-and-disaster-fraud.

[11] FBI. Elder Fraud, 2023. on-line at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/elder-fraud.

[12] FBI. Spoofing and Phishing, 2023. on-line at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing.

[13] Edwin Donald Frauenstein and Stephen Flowerday. Susceptibility to phishing on social network sites: A personality information processing model. *Computers & security*, 94:101862, 2020.

[14] Draško Grbić, Brankica Jokić, and Tatjana Medarević. *Osnovi informatike za šesti razred osnovne škole.* Zavod za udžbenike i nastavna sredstva, Istočno Sarajevo, 2014.

[15] Indeed. 17 Common Job Scams and How To Protect Yourself. on-line at: https://www.indeed.com/career-advice/finding-a-job/job-scams.

[16] Investopedia. Watch Out for These Top Internet Scams. on-line at: https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp.

[17] Svetlana Ignjatijević Jelena Matijašević, Žaklina Spalević. Vrste internet prevara - pojam, značaj i uticaj na ekonomske i moralne aspekte društvene zajednice. *INFOTEH-JAHORINA*, 2012.

[18] Kaspersky. What Is Pharming and How to Protect Yourself? on-line at: https://www.kaspersky.com/resource-center/definitions/pharming.

[19] Rashid Khan Mayur Bhati. Prevention approach of phishing on different websites. *International Journal of Engineering and Technology*, 2(7):1097–1098, 2015.

[20] New Hampshire Department of Justice. Don't Cash That Check! Check Overpayment Scams, 2023. on-line at: https://www.doj.nh.gov/consumer/dont-cash-that-check/check-overpayment.htm.

[21] Office of the Attorney General for the District of Columbia. Consumer Alert: Sweepstakes and Lottery Scams. on-line at: https://oag.dc.gov/consumer-protection/consumer-alert-sweepstakes-and-lottery-scams.

[22] Australian Federal Police. Internet Fraud. on-line at: https://www.police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf.

[23] New Zealand Police. Scams and fraud. on-line at: https://www.police.govt.nz/advice/email-and-internet-safety/internet-scams-spam-and-fraud.

[24] Proofpoint. What Is Catfishing? on-line at: https://www.proofpoint.com/us/threat-reference/catfishing.

[25] Vaggelis Saprikis, Adamantia Chouliara, and Maro Vlachopoulou. Perceptions towards online shopping: Analyzing the greek university students' attitude. *Communications of the IBIMA*, 2010, 2010.

[26] Panda Security. What Is DNS Spoofing and How Can You Prevent It? on-line at: https://www.pandasecurity.com/en/mediacenter/dns-spoofing.

[27] Federal trade commition. IdentityTheft. on-line at: https://www.ftc.gov/news-events/topics/identity-theft.

[28] Federal trade commition. Phishing scams and how to spot them. on-line at: https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams.

[29] Federal trade commition. What To Know About Cryptocurrency and Scams , 2022. on-line at: https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams#scams.

[30] Arun Vishwanath. Habitual facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, 20(1):83–98, 2015.

[31] Monica Therese Whitty. Is there a scam for everyone? psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research*, 26(3):399–409, 2020.

[32] Emma J Williams, Amy Beardmore, and Adam N Joinson. Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72:412–421, 2017.